

CLAIMS

What is claimed is:

- 1 1. A method for managing program data, comprising:
2 descrambling content in the program data; and
3 re-scrambling the content with a local key for future access to the content.
- 1 2. The method of claim 1 further comprising encrypting the local key with a unit
2 key and inserting the encrypted key into the program data for future access.
- 1 3. The method of claim 1 where the local key is a locally generated random number.
- 1 4. A method for managing program data, comprising:
2 deriving a code word needed to descramble content in the program data;
3 re-scrambling the code word with a local key; and
4 inserting the code word that was re-scrambled with the local key into the program
5 data for future access to the content.
- 1 5. The method of claim 4 further comprising inserting modified access criteria in
2 addition to the re-scrambled code word.
- 1 6. The method of claim 4 further comprising encrypting the local key with a unit
2 key and inserting the encrypted key into the program data for future access.
- 1 7. The method of claim 4 where the local key is a locally generated random number.
- 1 8. The method of claim 4 wherein the process, once initialized, is performed
2 essentially without CPU intervention.
- 1 9. The method of claim 6 further comprising packaging the encrypted key as an
2 entitlement management message prior to insertion into the program data for future
3 access.

- 1 10. A method for managing program data, comprising:
2 descrambling parameters used to derive a code word needed to descramble
3 content in the program data;
4 re-scrambling the parameters with a local key; and
5 inserting the parameters that were re-scrambled with the local key into the
6 program data for future access to the program data.
- 1 11. The method of claim 10 wherein some of the parameters are modified.
- 1 12. The method of claim 10 further comprising encrypting the local key with a unit
2 key and inserting the encrypted key into the program data for future access.
- 1 13. The method of claim 10 where the local key is a locally generated random
2 number.
- 1 14. The method of claim 12 further comprising packaging the encrypted key that as
2 an entitlement management message prior to insertion into the program data for future
3 access.
- 1 15. The method of claim 4 further comprising deriving a code word from an
2 entitlement control message, replacing certain fields of the entitlement control message
3 with new parameters and the code word that was re-scrambled with the local key, and
4 replacing the entitlement control message with the modified version of the entitlement
5 control message in the program data.
- 1 16. The method of claim 15 wherein the method, once initialized, is performed
2 essentially without CPU intervention.
- 1 17. The method of claim 4 further comprising identifying a packet with an
2 entitlement management message.

- 1 18. The method of claim 17 further comprising blanking data in the entitlement
2 management message.
- 1 19. The method of claim 17 further comprising inserting the local key into the
2 entitlement management message.
- 1 20. The method of claim 14 further comprising deriving the key from the entitlement
2 management message.
- 1 21. A computer-readable medium having stored thereon a sequence of instructions,
2 the sequence of instructions including instructions which, when executed by a processor,
3 causes the processor to perform a method comprising:
4 deriving a code word in an entitlement control message in program data with a
5 key;
6 re-scrambling the code word with a local key; and
7 inserting the re-scrambled code word into the entitlement control message.
- 1 22. The computer readable medium of claim 21, further comprising instructions
2 which, when executed by the processor, causes the processor to blank data in the
3 entitlement control message before inserting the code word.
- 1 23. The computer readable medium of claim 22, further comprising instructions
2 which, when executed by the processor, causes the processor to perform identifying a
3 packet with the entitlement control message.
- 1 24. The computer readable medium of claim 23, wherein identifying the packet with
2 the entitlement control message comprises sorting the program data according to packet
3 identifiers.
- 1 25. The computer readable medium of claim 21, further comprising instructions
2 which, when executed by the processor, causes the processor to perform identifying a
3 packet with an entitlement management message.

1 26. The computer readable medium of claim 25, further comprising instructions
2 which, when executed by the processor, causes the processor to perform blanking data in
3 the entitlement management message.

1 27. The computer readable medium of claim 25, further comprising instructions
2 which, when executed by the processor, causes the processor to perform inserting the
3 local key into the entitlement management message.

1 28. The computer readable medium of claim 25, further comprising instructions
2 which, when executed by the processor, causes the processor to perform deriving the key
3 from the entitlement management message.

1 29. A conditional access unit, comprising:
2 a control word descrambler unit that descrambles a control word from an
3 entitlement control message with a key;
4 a control word re-scrambling unit, coupled to the control word descrambler unit,
5 that re-scrambles the control word with a local key; and
6 a entitlement control message injector unit, coupled to the control word re-
7 scrambler unit, that injects the control word that has been re-scrambled with the local key
8 into the entitlement control message.

1 30. The conditional access unit of claim 29, wherein the conditional access unit is
2 managed essentially without CPU involvement.

1 31. The conditional access unit of claim 29 further comprising an entitlement control
2 message blanking unit, coupled to the entitlement control message injector unit, that
3 blanks data in the entitlement control message before transmitting the entitlement control
4 message to the entitlement control message injector unit.

1 32. The conditional access unit of claim 29, further comprising an entitlement
2 management message injector unit, that injects the local key into an entitlement
3 management message.

1 33. The conditional access unit of claim 32, further comprising an entitlement
2 management message blanking unit, coupled to the entitlement management message
3 injector unit, that blanks data in the entitlement management message before transmitting
4 the entitlement management message to the entitlement management message injector
5 unit.